Załącznik nr 1 do Zarządzenia Nr 8

z dnia 21 marca 2012 r.

**POLITYKA BEZPIECZEŃSTWA**

**PRZETWARZANIA DANYCH OSOBOWYCH**

**W ZESPOLE SZKÓŁ W ŻELISTRZEWIE**

SPIS TREŚCI

**ROZDZIAŁ I Postanowienia ogólne**

**ROZDZIAŁ II Wykaz zbiorów danych osobowych**

**ROZDZIAŁ III Wykaz pomieszczeń, w których przetwarzane są dane osobowe**

**ROZDZIAŁ IV Ewidencja osób upoważnionych do przetwarzania danych osobowych**

**ROZDZIAŁ V Opis zdarzeń naruszających ochronę danych osobowych**

**ROZDZIAŁ VI Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych zdarzeń**

Podstawa prawna:

* Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926)
* Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 3 listopada 2006r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2006, Nr 203, poz. 1494) – art. 13.3 ustawy
* Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2004 r. Nr 94, poz. 923) – art. 22a ustawy
* Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024) – art. 39a ustawy
* Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. nr 229, poz. 1536) – art. 46a ustawy.

**ROZDZIAŁ I**

**Postanowienia ogólne**

**§ 1.** 1. Polityka bezpieczeństwa przetwarzania danych osobowych w Zespole Szkół w Żelistrzewie zwana dalej „Polityką bezpieczeństwa”, określa podstawowe zasady dotyczące zapewnienia bezpieczeństwa w zakresie danych osobowych przetwarzanych w zbiorach danych:

1. tradycyjnych, w szczególności kartotekach, księgach, skorowidzach, aktach

osobowych, wykazach, w zbiorach ewidencyjnych;

1. w systemach informatycznych, w szczególności deklaracje ZUS, ewidencje

płacowe, stypendialne, informacje skarbowe, ewidencje statystyczne, plany

organizacyjne.

2. Ilekroć w Polityce Bezpieczeństwa jest mowa o:

1. ustawie – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie

danych osobowych z dnia 29 sierpnia 1997r. (tekst jedn. Dz. U. z 2002 r. Nr 101,

poz. 926 z późn. zm.);

1. administrator danych osobowych – rozumie się Dyrektora Zespołu Szkół w Żelistrzewie;
2. lokalny administrator danych osobowych – rozumie się pracownik administracyjnych szkoły, pedagoga, psychologa, logopedy, wychowawców, bibliotekarza, nauczycieli;
3. administrator sieci – rozumie się osobę odpowiedzialną za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemów

informatycznych, służących do przetwarzania danych osobowych;

1. nośniki danych osobowych – płyty CD lub DVD, pamięć flash, dyski twarde, taśmy magnetyczne lub inne urządzenia/ materiały służące do przechowywania plików z danymi;
2. osoba upoważniona (użytkownik) – osoba posiadająca upoważnienie wydane

przez administratora danych osobowych ;

1. Administrator Bezpieczeństwa Informacji – osoba powołana zarządzeniem

dyrektora, której zadaniem jest nadzorowanie i koordynowanie w szkole zasad

postępowania przy przetwarzaniu danych osobowych

1. dane osobowe - w rozumieniu ustawy za dane osobowe uważa się wszelkie

informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby

fizycznej;

1. przetwarzanie danych - rozumie się przez to jakiekolwiek operacje wykonywane

na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie,

opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

1. zbiór danych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów;
2. system informatyczny - zespół współpracujących ze sobą urządzeń, programów,

procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

1. identyfikator użytkownika (login) - ciąg znaków literowych, cyfrowych lub innych,

jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych

osobowych w systemie informatycznym;

1. hasło - ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systeminformatycznym;
2. uwierzytelnianie — rozumie się przez to działanie, którego celem jest weryfikacja

deklarowanej tożsamości podmiotu;

1. poufności danych — rozumie się przez to właściwość zapewniającą, że dane nie

są udostępniane nieupoważnionym podmiotom.

**§ 2.** 1. Dyrektor Zespołu Szkół w Żelistrzewie realizując politykę bezpieczeństwa dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:

1. przetwarzane zgodnie z prawem;
2. zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane przetwarzaniu niezgodnemu z tymi celami;
3. merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są

przetwarzane;

1. przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą.

2. Dyrektor Zespołu Szkół w Żelistrzewie dąży do systematycznego unowocześniania stosowanych na terenie szkoły informatycznych, technicznych i organizacyjnych środków ochrony tych danych w celu zabezpieczenia danych osobowych przed ich udostępnianiem osobom nieupoważnionym, przetwarzaniem z naruszeniem przepisów o ochronie danych osobowych, nieautoryzowaną zmianą, uszkodzeniem lub zniszczeniem.

**ROZDZIAŁ II**

**Wykaz zbiorów danych osobowych w Zespole Szkół w Żelistrzewie**

**§ 3.** Dane osobowe gromadzone są w zbiorach. Wykaz zbiorów danych osobowych stanowi

załącznik nr 4.

**§ 4**. Zbiory danych osobowych wymienione w załączniku nr 4 podlegają przetwarzaniu

w sposób tradycyjny.

**ROZDZIAŁ III**

**Wykaz pomieszczeń, w których przetwarzane są dane osobowe.**

**§ 5**. 1. Dane osobowe gromadzone i przetwarzane są w budynku szkolnym, mieszczącym

się w Żelistrzewie przy Szkolnej 1.

2. Obszarami do przetwarzania danych osobowych z użyciem sprzętu komputerowego oraz

sposobem ręcznym są pomieszczenia wskazane w załączniku nr 6.

3. Zabrania się przetwarzania danych poza obszarami wskazanymi określonym w załączniku

nr 6.

4. Przebywanie osób, nieuprawnionych w obszarach wskazanych w załączniku nr 6 w czasie

przetwarzania danych osobowych jest dopuszczalne za zgodą Administratora danych lub

w obecności osoby upoważnionej do przetwarzania danych osobowych – za jego zgodą.

Wzory zgody na przebywanie w pomieszczeniach dla osób nie posiadających upoważnienia,

a także odwołania tej zgody, stanowią odpowiednio załącznik nr 7 oraz załącznik nr 8 do

przedmiotowej dokumentacji.

**ROZDZIAŁ IV**

**Ewidencja osób upoważnionych do przetwarzania danych osobowych**

**§ 6**.1. Ewidencja osób, które mają dostęp do zbiorów danych osobowych stanowi załącznik

nr 3.

2. Ewidencja zawiera: imię i nazwisko osoby upoważnionej, datę nadania i ustania

uprawnień oraz zakres, a w przypadku kiedy dane są przetwarzane za pomocą programu

komputerowego również identyfikator dostępowy do tego programu.

3. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne

upoważnienie. Wzór upoważnienia stanowi załącznik nr 4. Prowadzi się ewidencję

upoważnień.

4. Unieważnienie upoważnienia następuje na piśmie, wg wzoru stanowiącego załącznik nr 5.

5. Każdy upoważniony do przetwarzania danych potwierdza pisemnie fakt zapoznania się

z niniejszą dokumentacją i zrozumieniem wszystkich zasad bezpieczeństwa. Wzór

potwierdzenia stanowi załącznik nr 6. Podpisany dokument jest dołączany do akt

osobowych.

**ROZDZIAŁ V**

**Opis zdarzeń naruszających ochronę danych osobowych**

**§ 7**. Rodzaje zagrożeń naruszających ochronę danych osobowych:

1. Zagrożenia losowe:

1) zewnętrzne np. klęski żywiołowe, przerwy w zasilaniu – ich wystąpienie może

prowadzić do utraty integralności danych lub ich zniszczenia lub uszkodzenia

infrastruktury technicznej systemu: ciągłość zostaje naruszona, jednak nie dochodzi

do naruszenia danych osobowych;

2) wewnętrzne np. niezamierzone pomyłki operatorów, awarie sprzętowe, błędy oprogramowania – w wyniku ich wystąpienia może dojść do zniszczenia danych, może nastąpić zakłócenie ciągłości pracy systemu i naruszenia poufności danych.

2. Zagrożenia zamierzone (świadome i celowe naruszenia poufności danych) – w wyniku ich

wystąpienia zazwyczaj nie występuje uszkodzenie infrastruktury technicznej i zakłócenie

ciągłości pracy. W ramach tej kategorii zagrożeń wystąpić mogą:

1. nieuprawniony dostęp do systemu z zewnątrz;
2. nieuprawniony dostęp do systemu z wewnątrz;
3. nieuprawnione przekazanie danych;
4. bezpośrednie zagrożenie materialnych składników np. kradzież, zniszczenie.

3. Okoliczności zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia

zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to

w szczególności:

1. sytuacje losowe lub nieprzewidywalne oddziaływanie czynników zewnętrznych na

zasoby systemu np. wybuch gazu, pożar, zalanie pomieszczeń, uszkodzenia wskutek

prowadzonych prac remontowych;

1. niewłaściwe parametry środowiska np. nadmierna wilgotność, temperatura, wstrząsy,

oddziaływania pola elektromagnetycznego, przeciążenia napięcia;;

1. awarie sprzętu lub oprogramowania, które są celowym działaniem na potrzeby

naruszenia ochrony danych osobowych;

1. pojawienie się odpowiedniego komunikatu alarmowego od części systemu, która

zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu ;

1. pogorszenie jakości danych w systemie lub inne odstępstwo od stanu oczekiwanego

wskazujące na zakłócenia systemu lub niepożądaną modyfikację w systemie;

1. naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym

systemie;

1. modyfikacja danych lub zmiana w strukturze danych bez odpowiedniego

upoważnienia;

1. ujawnienie osobom nieuprawnionym danych osobowych lub objętych tajemnicą

procedur ochrony ich przetwarzania;

1. podmienienie lub zniszczenie nośników z danymi osobowymi bez odpowiedniego

upoważnienia lub skasowanie bądź skopiowanie w sposób niedozwolony danych

osobowych;

1. rażące naruszenie obowiązków w zakresie przestrzegania procedur bezpieczeństwa

informacji (niewylogowywanie się przed opuszczeniem stanowiska pracy,

pozostawienie danych w drukarce lub kserokopiarce, niewykonanie kopii zapasowych,

prace na danych osobowych w celach prywatnych itp.);

1. nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych

osobowych, znajdujących się na dyskach, płytach CD, kartach pamięci oraz

wydrukach komputerowych w formie niezabezpieczonej (otwarte szafy, biurka, regały, archiwum).

4. W przypadku stwierdzenia naruszenia zasad bezpieczeństwa danych osobowych

sporządza się raport zgodnie ze wzorem będącym załącznikiem nr 9 oraz przedstawienia

się go Administratorowi danych.

**ROZDZIAŁ VI**

**Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności,**

**integralności i rozliczalności przetwarzania danych osobowych**

**§ 8.** 1. Formy zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe:

1. wszystkie pomieszczenia, w których przetwarzane są dane osobowe zamykane są na

klucz, w przypadku opuszczenia przez ostatnia osobę upoważnioną do przetwarzania

danych osobowych – także w godzinach pracy;

1. dane osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej

(pamięć flash, płyty CD, DVD, dyskietki) po zakończeniu pracy są przechowywane w zamykanych na klucz meblach biurowych, a tam, gdzie jest to możliwe w szafach

1. pancernych lub metalowych;

nieaktualne lub błędne wydruki zawierające dane osobowe niszczone są w niszczarkach;

1. budynek, w którym są przetwarzane dane jest chroniony systemem alarmowym

z telefonicznym powiadamianiem oraz całodobowym systemem monitoringu na

zewnątrz budynku.

**§ 9.** 1. Formy zabezpieczeń przed nieautoryzowanym dostępem do danych osobowych:

1. podłączenie urządzenia końcowego (komputera, drukarki) do sieci komputerowej

Zespołu Szkół w Żelistrzewie dokonywane jest przez administratora sieci;

1. udostępnianie użytkownikowi zasobów sieci zawierających dane osobowe przez

administratora sieci następuje na podstawie upoważnienia do przetwarzania danych

osobowych;

1. identyfikacja użytkownika w systemie następuje poprzez zastosowanie uwierzytelniania (login, hasło; dot. danych przetwarzanych przy użyciu systemu

informatycznego);

1. udostępnianie kluczy do pomieszczeń, w których przetwarzane są dane osobowe
2. tylko osobom upoważnionym; ustawienie monitorów na stanowiskach pracy w sposób uniemożliwiający wgląd w dane osobowe (dot. danych przetwarzanych przy użyciu systemu informatycznego).
3. wymuszenie zmiany hasła np. co 30 dni (SIO, Hermes).

**§ 10.** 1. Formy zabezpieczeń przed utratą danych osobowych w wyniku awarii:

1. odrębne zasilanie sprzętu komputerowego lub zastosowanie zasilaczy zapasowych

UPS – komputer głównej księgowej;

1. zastosowanie ochrony antywirusowej – komputery: w gabinecie dyrektora, sekretariacie oraz w księgowości;
2. zapewnienie właściwej temperatury i wilgotności w pomieszczeniach.

**§ 11.** 1. Organizację ochrony danych osobowych realizuje się poprzez:

1. zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych przed dopuszczeniem do pracy;
2. kontrolowanie pomieszczeń budynku;
3. prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
4. wyznaczenie Administratora Bezpieczeństwa Informacji.

INSTRUKCJA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

W ZESPOLE SZKÓŁ W ŻELISTRZEWIE

**§ 1**. 1. Nadawanie uprawnień do przetwarzania danych oraz ich rejestrowanie

w systemie informatycznym.

1. Do obsługi systemu informatycznego służącego do przetwarzania danych

osobowych, może być dopuszczona wyłącznie osoba posiadająca upoważnienie

do przetwarzania danych osobowych, wydane przez Administratora danych

osobowych.

1. Upoważnienia do przetwarzania danych osobowych, przechowywane są w teczkach akt osobowych pracowników oraz prowadzona jest ich ewidencja.
2. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może

mieć miejsce wyłącznie po :

1. podaniu identyfikatora użytkownika i właściwego hasła w przypadku obsługi

SIO, HERMES, Płatnik;

1. podaniu właściwego hasła dostępu do stanowiska komputerowego

w przypadku obsługi OFFICE, VULCAN.

1. Dla każdego użytkownika systemu informatycznego, który przetwarza dane

osobowe, Administrator Bezpieczeństwa Informacji ustala niepowtarzalny

1. identyfikator i hasło początkowe.

Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu

użytkownika z systemu informatycznego, nie powinien być przydzielany innej

osobie.

1. W przypadku utraty przez daną osobę uprawnień do dostępu do danych

osobowych w systemie informatycznym. Identyfikator osoby, która utraciła

uprawnienia do dostępu do danych osobowych, należy niezwłocznie

wyrejestrować z systemu informatycznego, unieważnić jej hasło, oraz podjąć inne

stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych.

Za realizację procedury rejestrowania i wyrejestrowywanie użytkowników w

systemie informatycznym odpowiedzialny jest Administrator Bezpieczeństwa

Informacji.

**§ 2**. 1. Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem

i użytkowaniem.

1. Dane osobowe przetwarzane są z użyciem serwerów, komputerów stacjonarnych
2. Hasło użytkownika powinno mieć minimum 8 znaków i być zmieniane w przypadku :
   1. Systemu SIO, HERMES, Płatnik – co 30 dni,
   2. zmiana hasła dostępu do stanowiska komputerowego co 90 dni.
3. Hasło oprócz znaków małych i dużych liter winno zawierać ciąg znaków

alfanumerycznych i specjalnych;

1. Hasła wpisywane z klawiatury nie mogą pojawiać się na ekranie monitorów w formie

jawnej;

1. Hasło nie może zawierać żadnych informacji, które można kojarzyć z użytkownikiem

komputera np. osobiste dane użytkownika, tj. nazwisko, inicjały, imiona, marka lub nr

rejestracyjny samochodu itp.;

1. Hasło nie może być zapisywane w miejscu dostępnym dla osób nieuprawnionych.

Użytkownik nie może udostępnić swojego identyfikatora oraz hasła jak również

dostępu do stanowiska roboczego po uwierzytelnieniu w systemie osobom

nieuprawnionym ani żadnej osobie postronnej;

1. Hasło użytkownika, umożliwiające dostęp do systemu informatycznego, należy

utrzymywać w tajemnicy, również po upływie jego ważności;

1. Raz użyty identyfikator nie może być przydzielony innemu użytkownikowi;
2. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona,

użytkownik zobowiązany jest do natychmiastowej zmiany hasła, lub w razie

problemów powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji.

**§ 3**. 1. Procedury rozpoczęcia, zawieszenia i zakończenia pracy.

1. Dane osobowe, których administratorem jest szkoła mogą być przetwarzane

sposobem tradycyjnym lub z użyciem systemu informatycznego tylko na potrzeby

1. realizowania zadań statutowych i organizacyjnych szkoły;

Rozpoczęcie pracy użytkownika w systemie informatycznym następuje po

poprawnym uwierzytelnieniu (zalogowaniu się do systemu);

1. Rozpoczęcie pracy w aplikacji musi być przeprowadzone zgodnie z instrukcją

zawartą w dokumentacji aplikacji;

1. Zakończenie pracy użytkownika następuje po poprawnym wylogowaniu się

z systemu oraz poprzez uruchomienie odpowiedniej dla danego systemu opcji jego

zamknięcia zgodnie z instrukcją zawartą w dokumentacji;

1. Niedopuszczalne jest zakończenie pracy w systemie bez wykonania pełnej i

poprawnej operacji wylogowania z aplikacji i poprawnego zamknięcia systemu;

1. Monitory stanowisk komputerowych znajdujące się w pomieszczeniach, gdzie

przebywają osoby, które nie posiadają upoważnień do przetwarzania danych

osobowych, a na których przetwarzane są dane osobowe należy ustawić w taki

sposób, aby uniemożliwić osobom postronnym wgląd w dane;

1. Użytkownik ma obowiązek wylogowania się w przypadku zakończenia pracy.

Stanowisko komputerowe nie może pozostać z uruchomionym i dostępnym

systemem bez nadzoru pracującego na nim pracownika;

1. Wydruki zawierające dane osobowe należy przechowywać w miejscu

uniemożliwiającym ich odczytanie przez osoby postronne. Wydruki nieprzydatne

należy zniszczyć w stopniu uniemożliwiającym ich odczytanie w niszczarce

1. dokumentów;

Przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się na

obszarze, w którym są przetwarzane dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania;

1. Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać, na czas

nieobecności osób zatrudnionych, w sposób uniemożliwiający dostęp do nich

osobom trzecim;

1. Użytkownik niezwłocznie powiadamia Administratora Bezpieczeństwa Informacji

w przypadku podejrzenia fizycznej ingerencji w przetwarzane dane osobowe lub

użytkowane narzędzia programowe lub sprzętowe. Wówczas, użytkownik jest

zobowiązany do natychmiastowego wyłączenia sprzętu.

**§ 4**. 1. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów

i narzędzi do ich przetwarzania.

1. Zbiory danych osobowych w systemie informatycznym są zabezpieczane przed

utratą lub uszkodzeniem za pomocą:

1. urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci

zasilającej,

1. sporządzanie kopii zapasowych (kopie pełne).
2. Kopie zapasowe zbiorów danych tworzone są: w przypadku SIO – 3 x w ciągu roku,

Hermes – 1 x w ciągu roku, SIGMA 1x w ciągu miesiąca;

1. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich

przydatności do odtworzenia w przypadku awarii systemu. Za przeprowadzenie tych

czynności odpowiada Administrator Bezpieczeństwa Informacji;

1. Nośniki danych po ustaniu ich użyteczności należy pozbawić danych lub zniszczyć

w sposób uniemożliwiający odczyt danych.

**§ 5**. 1. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji

zawierających dane osobowe oraz kopii zapasowych

1. Okresowe kopie zapasowe wykonywane są na płytach CD lub innych

elektronicznych nośnikach informacji. Kopie zapasowe przechowuje się w sposób

uniemożliwiający nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie

w kasie pancernej pomieszczeniu dyrektora szkoły.

1. Dostęp do nośników z kopiami zapasowymi systemu oraz kopiami danych

osobowych, ma wyłącznie Administrator Bezpieczeństwa Informacji .

1. Kopie przechowuje się przez okres 2 lat. Kopie zapasowe należy bezzwłocznie

usuwać po ustaniu ich użyteczności.

1. Usunięcie danych z systemu powinno zostać zrealizowane przy pomocy

oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika

informacji.

1. W przypadku kopii zapasowych sporządzanych indywidualnie przez użytkownika

odpowiedzialnością za ich zniszczenie obarczony jest użytkownik.

1. W przypadku nośników informacji, przez ich zniszczenie rozumie się ich trwałe

i nieodwracalne zniszczenie fizyczne do stanu nie dającego możliwości ich

rekonstrukcji i odzyskania danych.

**§ 6**. 1. Sposób zabezpieczenia systemu informatycznego przed działaniem

oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu

informatycznego

1. W związku z istnieniem zagrożenia dla zbiorów danych osobowych, ze strony

wirusów komputerowych, których celem jest uzyskanie nieuprawnionego dostępu do

systemu informatycznego, konieczna jest ochrona sieci komputerowej i stanowisk

komputerowych.

1. Wirusy komputerowe mogą pojawić się systemach szkoły poprzez: Internet, nośniki

informacji takie jak: dyskietki, płyty CD, dyski przenośne, itp.

1. Przeciwdziałanie zagrożeniom ze strony wirusów komputerowych realizowane jest

następująco:

1. Komputer z dostępem do Internetu musi być zabezpieczony za pomocą

oprogramowania antywirusowego.

1. Zainstalowany program antywirusowy powinien być tak skonfigurowany, by co

najmniej raz w tygodniu dokonywał aktualizacji bazy wirusów oraz co najmniej

raz w tygodniu dokonywane było automatycznie sprawdzenie komputera pod

kątem obecności wirusów komputerowych.

1. Elektroniczne nośniki informacji takie jak dyskietki, dyski przenośne, należy

każdorazowo sprawdzać programem antywirusowym przed użyciem, po

zainstalowaniu ich w systemie. Czynność powyższą realizuje użytkownik

systemu. W przypadku problemów ze sprawdzeniem zewnętrznego nośnika

danych użytkownik jest zobowiązany zwrócić się z tym do Administratora

Bezpieczeństwa Informacji.

1. Komputery i systemy pracujące muszą mieć zainstalowany program

antywirusowy a w przypadku komputerów z dostępem do Internetu, również

posiadać oprogramowanie i mechanizmy zabezpieczające przed

nieautoryzowanym dostępem z sieci (firewall).

1. W przypadku, gdy użytkownik stanowiska komputerowego zauważy komunikat

oprogramowania zabezpieczającego system wskazujący na zaistnienie

zagrożenia lub rozpozna tego typu zagrożenie, zobowiązany jest zaprzestać

jakichkolwiek czynności w systemie i niezwłocznie skontaktować się

z Administratorem Bezpieczeństwa Informacji.

1. Przy korzystaniu z poczty elektronicznej należy zwrócić szczególną uwagę na

otrzymywane załączniki dołączane do treści wiadomości. Zabrania się

otwierania załączników i wiadomości poczty elektronicznej od „niezaufanych”

nadawców.

1. Zabrania się użytkownikom komputerów, wyłączania, blokowania

odinstalowywania programów zabezpieczających komputer (skaner

antywirusowy, firewall) przed oprogramowaniem złośliwym oraz

nieautoryzowanym dostępem.

**§ 7**. Udostępnianie danych osobowych i sposób odnotowania informacji

o udostępnionych danych

7.1. Udostępnienie danych instytucjom może odbywać się wyłącznie na pisemny

uzasadniony wniosek lub zgodnie z przepisami prawa (OKE, CKE, Urząd Gminy, itp.).

**§ 8**. Wykonywanie przeglądów i konserwacji systemu oraz nośników informacji

służących do przetwarzania danych

8.1. Przeglądy i konserwacje systemu oraz zbiorów danych wykonuje Administrator

Bezpieczeństwa Informacji na bieżąco.

8.2. Administrator Bezpieczeństwa Informacji okresowo sprawdza możliwość odtworzenia

danych z kopii zapasowej.

8.3. Umowy dotyczące instalacji i konserwacji sprzętu należy zawierać z podmiotami, których

kompetencje nie budzą wątpliwości, co do wykonania usługi oraz których wiarygodność

finansowa zostały sprawdzone na rynku.

8.4. Naprawy sprzętu należy zlecać podmiotom, których kompetencje nie budzą wątpliwości,

co do wykonania usługi. Naprawa sprzętu, na którym mogą znajdować się dane

osobowe powinna odbywać się pod nadzorem osób użytkujących sprzęt oraz

Administratora Bezpieczeństwa Informacji w miejscu jego użytkowania.

8.5. W przypadku konieczności naprawy poza miejscem użytkowania, sprzęt komputerowy,

przed oddaniem do serwisu, powinien być odpowiednio przygotowany. Dane należy

zarchiwizować na nośniki informacji, a dyski twarde, bezwzględnie, wymontować na

czas naprawy.

8.6. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub

zmiana jego lokalizacji, może być dokonana tylko za wiedzą i zgodą Administratora

Bezpieczeństwa Informacji.

**§ 9**. Ustalenia końcowe

9.1. Osobom korzystającym z systemu informatycznego, w którym przetwarzane

są dane osobowe w szkole zabrania się:

* 1. ujawniania loginu i hasła współpracownikom i osobom z zewnątrz,
  2. pozostawiania haseł w miejscach widocznych dla innych osób,
  3. udostępniania stanowisk pracy wraz z danymi osobowymi osobom nieuprawnionym,
  4. udostępniania osobom nieuprawnionym programów komputerowych

zainstalowanych w systemie,

* 1. używania oprogramowania w innym zakresie niż pozwala na to umowa licencyjna,
  2. przenoszenia programów komputerowych, dysków twardych z jednego stanowiska na inne,
  3. kopiowania danych na nośniki informacji, kopiowania na inne systemy celem

wynoszenia ich poza szkołę,samowolnego instalowania i używania jakichkolwiek programów komputerowych w tym również programów do użytku prywatnego; programy komputerowe

* 1. instalowane są przez Administratora Bezpieczeństwa Informacji,
  2. używania nośników danych udostępnionych przez osoby postronne,
  3. przesyłania dokumentów i danych z wykorzystaniem konta pocztowego prywatnego (niesłużbowego),
  4. otwierania załączników i wiadomości poczty elektronicznej od nieznanych

i „niezaufanych” nadawców,

* 1. używania nośników danych niesprawdzonych, niewiadomego pochodzenia lub

niezwiązanych z wykonywaną pracą; w przypadku konieczności użycia

niesprawdzonych przenośnych nośników danych, należy zgłosić te nośniki, w celu sprawdzenia - przeskanowania programem antywirusowym, Administratorowi Bezpieczeństwa Informacji,

* 1. tworzenia kopii zapasowych niechronionych hasłem i/lub bez odpowiednich

zabezpieczeń miejsca ich przechowywania.

9.2. Ponadto zabrania się:

* 1. wyrzucania dokumentów zawierających dane osobowe bez uprzedniego ich

trwałego zniszczenia,

* 1. pozostawiania dokumentów, kopii dokumentów zawierających dane osobowe

w drukarkach, kserokopiarkach,

* 1. pozostawiania kluczy w drzwiach, szafach, biurkach, zostawiania otwartych

pomieszczeń, w których przetwarza się dane osobowe,

* 1. pozostawiania bez nadzoru osób trzecich przebywających w pomieszczeniach

szkoły, w których przetwarzane są dane osobowe,

* 1. pozostawiania dokumentów na biurku po zakończonej pracy, pozostawiania

otwartych dokumentów na ekranie monitora bez blokady konsoli,

* 1. ignorowania nieznanych osób z zewnątrz poruszających się w obszarze

przetwarzania danych osobowych,

* 1. przekazywania informacji będącymi danymi osobowymi osobom nieupoważnionym,
  2. ignorowania zapisów Polityki Bezpieczeństwa szkoły.

9.3. Konieczne jest:

1. posługiwanie się własnym loginem i hasłem w celu uzyskania dostępu do systemów

informatycznych,

1. tworzenia haseł trudnych do odgadnięcia dla innych,
2. traktowanie konta pocztowego szkoły jako narzędzia pracy i wykorzystywanie go

jedynie w celach służbowych,

1. nie przerywanie procesu skanowania przez program antywirusowy na komputerze,
2. wykonywanie kopii zapasowych danych przetwarzanych na stanowisku

komputerowym,

1. zabezpieczenie sprzętu komputerowego przed kradzieżą lub nieuprawnionym

dostępem do danych.

9.4. Wszelkie przypadki naruszenia niniejszej Instrukcji należy zgłaszać Administratorowi

Bezpieczeństwa Informacji lub bezpośredniemu przełożonemu.

**§ 10.** Zalecenia w zakresie przetwarzania danych osobowych sposobem tradycyjnym

1. Miejscem tworzenia, uzupełniania, przechowywania dokumentacji dotyczącej

przetwarzania danych osobowych sposobem tradycyjnym są pomieszczenia

wskazane w załączniku nr 2.

1. Miejscem tworzenia, uzupełniania, przechowywania dokumentacji dotyczącej

przetwarzania danych osobowych przy użyciu systemu informatycznego są

pomieszczenia wskazane w załączniku nr 2 pkt. 1, 2, 3.

1. Osoby prowadzące dokumentację zobowiązane są do zachowania tajemnicy

służbowej.

1. Dokumentacji, o której mowa w punkcie 1 nie można wynosić poza teren szkoły,

kopiować itp.

1. Dokumentację, o której mowa w punkcie 1 archiwizuje się zgodnie z Instrukcją

kancelaryjną.

1. Osoby prowadzące dokumentację zobowiązane są do niezwłocznego

poinformowania Administratora Bezpieczeństwa Informacji o podejrzeniu dostępu do

dokumentacji przez osoby nieupoważnione.

**§ 11.** Obowiązki Administratora Danych

1. Administrator danych zobowiązany jest do zapewnienia, aby dane osobowe były:

1. przetwarzane zgodnie z prawem,
2. zbierane dla oznaczonych, zgodnych z prawem celów,
3. merytorycznie poprawne i adekwatne w stosunku do celów.

2. Wyznacza osobę, zwaną dalej Administratorem Bezpieczeństwa Informacji,

odpowiedzialnym za bezpieczeństwo danych osobowych w systemie informatycznym,

w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu,

w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań

w przypadku wykrycia naruszeń w systemie zabezpieczeń.

3. Opracowuje instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych,

przeznaczoną dla osób zatrudnionych przy przetwarzaniu tych danych.

4. Określa budynki, pomieszczenia lub części pomieszczeń, tworzące obszar, w którym

przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego.

5. Prowadzi ewidencję osób uprawnionych do przetwarzania danych osobowych

w poszczególnych systemach.

6. Organizuje szkolenia mające na celu zaznajomienie każdej osoby przetwarzającej dane

osobowe z przepisami dotyczącymi ich ochrony.

7. Odpowiada za to by zakres czynności osoby zatrudnionej przy przetwarzania danych

osobowych określał odpowiedzialność tej osoby za:

* 1. ochronę danych przed niepowołanym dostępem,
  2. nieuzasadnioną modyfikację lub zniszczenie danych,
  3. nielegalne ujawnienie danych w stopniu odpowiednim do zadań realizowanych w procesie przetwarzania danych osobowych.

**§ 12.** Obowiązki Administratora Bezpieczeństwa Informacji

1. Nadzór nad przestrzeganiem instrukcji określającej sposób zarządzania systemem

informatycznym.

2. Nadzór nad właściwym zabezpieczeniem sprzętu oraz pomieszczeń, w których

przetwarzane są dane osobowe.

3. Nadzór nad wykorzystywanym w szkole oprogramowaniem oraz jego legalnością.

4. Przeciwdziałanie dostępowi osób niepowołanych do systemu, w których przetwarzane są

dane osobowe.

5. Podejmowanie odpowiednich działań w celu właściwego zabezpieczenia danych.

6. Badanie ewentualnych naruszeń w systemie zabezpieczeń danych osobowych.

7. Podejmowanie decyzji o instalowaniu nowych urządzeń oraz oprogramowania

wykorzystywanego do przetwarzania danych osobowych.

8. Nadzór na naprawami, konserwacją oraz likwidacją urządzeń komputerowych

zawierających dane osobowe.

9. Definiowanie użytkowników i haseł dostępu.

10. Aktualizowanie oprogramowania antywirusowego i innego, chyba że aktualizacje te

wykonywane są automatycznie.

11. Nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym

sprawdzaniem pod kątem ich dalszej przydatności.

12. Sporządzanie raportów z naruszenia bezpieczeństwa systemu informatycznego.

Zatwierdził (data i podpis): ………………………………….

# Załącznik nr 1

……….……………..

*(data)*

…………………….……………...

*(imię i nazwisko pracownika)*

**Oświadczenie pracownika**

**zatrudnionego przy przetwarzaniu danych osobowych w zbiorach danych przetwarzanych przez Zespół Szkół w Żelistrzewie**

Obowiązki pracownika

**Pracownik dopuszczony do przetwarzania danych osobowych zobowiązany jest do:**

1. Zapoznania się i przestrzegania obowiązków wynikających z:
2. Przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz aktów wykonawczych wydanych na jej podstawie,
3. Dokumentów wprowadzonych przez Zespół Szkół w Żelistrzewie w związku z przetwarzaniem danych osobowych, w szczególności:

* Polityki Bezpieczeństwa Przetwarzania Danych Osobowych,
* Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych.

1. Zapewnienia bezpieczeństwa przetwarzania danych osobowych poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem.
2. Zachowania w tajemnicy danych oraz sposobu ich zabezpieczenia do których uzyskał dostęp w trakcie zatrudnienia, również po ustaniu zatrudnienia.

Odpowiedzialność pracownika

Za niedopełnienie obowiązków wynikających z niniejszego oświadczenia pracownik ponosi odpowiedzialność na podstawie przepisów Regulaminu pracy, Kodeksu pracy oraz Ustawy o ochronie danych osobowych.

**Oświadczam, że treść niniejszego oświadczenia jest mi znana i zobowiązuję się do jego przestrzegania.**

*Potwierdzam odbiór 1 egz. oświadczenia..*

..................................... ..........................................

pracownik pracodawca

**Załącznik nr 2 Wzór upoważnienia do przetwarzania danych osobowych**

**UPOWAŻNIENIE**

**DO PRZETWARZANIA DANYCH OSOBOWYCH**

Działając na podstawie art. 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (t.j.Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)

– udziela się Panu/Pani\*:

........................................................................................................................................

(imię i nazwisko pracownika)

........................................................................................................................................

(stanowisko służbowe)

upoważnienia do przetwarzania danych osobowych, których Administratorem Danych Zespołu Szkół oraz do przetwarzania danych osobowych ………………………..przez podmioty trzecie.

Jest Pan/Pani\* upoważniony/upoważniona\* do przetwarzania danych osobowych wyłącznie w zakresie wynikającym z Pana/Pani\* zadań oraz poleceń przełożonego.

Upoważnienie traci ważność z chwilą ustania stosunku pracy.

|  |  |
| --- | --- |
|  | ......................................................................  (data i podpis Administratora Bezpieczeństwa Informacji) |

\* niepotrzebne skreślić

# Załącznik nr 3 Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

**Ewidencja osób upoważnionych do przetwarzania danych osobowych**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **l.p.** | **Imię** | **Nazwisko** | **Komórka organizacyjna** | **Zakres upoważnienia** | **Identyfikator/nazwa systemu** | **Data nadania uprawnień** | **Data odebrania uprawnień** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

# Załącznik nr 4 Wykaz zbiorów danych osobowych oraz opis struktury zbiorów danych osobowych

1. **Wykaz zbiorów danych osobowych**
   1. Zbiór danych kadrowych (nauczyciele i inni pracownicy),
   2. Kandydaci do pracy,
   3. Ewidencja uczniów (obecnych i byłych) i związane z nimi dane rodziców,
   4. Zbiór danych uczniów z okręgu szkoły realizujących obowiązek szkolny w innych szkołach,
   5. Zbiór uczniów, którym przyznawane są stypendia za osiągnięcia
   6. Zamówienia publiczne,
   7. Ewidencja osób ubiegających się o uzyskanie informacji publicznej,
   8. Rejestr skarg i wniosków,
   9. Rejestr korespondencji,
   10. Archiwum zakładowe,
   11. Zbiór danych prowadzony w ramach systemu informacji oświatowej.
2. **Opis struktury zbiorów danych osobowych**
3. Nazwa zbioru: Zbiór danych kadrowych

Kategoria osób: nauczyciele i inni pracownicy

Dane identyfikujące: imię i nazwisko, adres, dane kontaktowe (np. nr tel. stacjonarnego lub komórkowego), data urodzenia, rysopis (np. zdjęcie), nr NIP, nr PESEL, seria i nr dowodu osobistego oraz stosunek do służby wojskowej.

Dane kontaktowe: imię i nazwisko, miejsce pracy, funkcja lub stanowisko, (ewentualnie nr certyfikatu) podpis, służbowy adres e-mail

Dane dotyczące wykształcenia oraz ukończonych kursów: poziom wykształcenia, data ukończenia szkoły, nazwa ukończonej szkoły w przypadku szkoły wyższej, typ ukończonej szkoły, profil, stopień (tytuł naukowo – zawodowy), specjalizacja, ukończone studia podyplomowe, ukończone kursy, ważniejsze szkolenia, posiadane uprawnienia, kwalifikacje, inne umiejętności, znajomość systemów informatycznych, stopień znajomości języków obcych,

Dane służące do reprezentacji: imię i nazwisko, miejsce pracy, funkcja lub stanowisko, (ewentualnie nr certyfikatu) podpis, służbowy adres e-mail, seria i nr dowodu osobistego

Dane dotyczące rodziny: stan cywilny, nazwisko panieńskie matki, imiona rodziców, imię i nazwisko oraz data urodzenia współmałżonka, imię i nazwisko, data urodzenia dziecka lub dzieci pracownika, imię i nazwisko, adres oraz nr telefonu osoby, która należy poinformować w razie wypadku pracownika

Dane dotyczące przebiegu zatrudnienia: adres do korespondencji, nazwisko panieńskie, obywatelstwo, przebieg kariery, czas pracy, dane dotyczące zdolności do pracy, informacje o nr rachunku bankowego, wysokość wynagrodzenia, nagrody, premie, kwoty udzielonych pożyczek, informacje o zatrudnieniu u innego pracodawcy

Dane dotyczące ubezpieczenia społecznego i zdrowotnego: informacje o oddziale Narodowego Funduszu Zdrowia

Dane dotyczące karalności: oświadczenie o ukaraniu sądowym

1. Nazwa zbioru:

Kategoria osób:

Dane kontaktowe: imię i nazwisko, miejsce pracy, funkcja lub stanowisko, (ewentualnie nr certyfikatu) podpis, służbowy adres e-mail

1. Nazwa zbioru:

Kategoria osób:

Dane identyfikujące: imię i nazwisko, adres, dane kontaktowe (np. nr tel. stacjonarnego lub komórkowego), data urodzenia, rysopis (np. zdjęcie), nr NIP, nr PESEL, seria i nr dowodu osobistego oraz stosunek do służby wojskowej.

Dane kontaktowe: imię i nazwisko, miejsce pracy, funkcja lub stanowisko, (ewentualnie nr certyfikatu) podpis, służbowy adres e-mail

1. Nazwa zbioru:

Kategoria osób:.

Dane identyfikujące: imię i nazwisko, adres, dane kontaktowe (np. nr tel. stacjonarnego lub komórkowego), data urodzenia, rysopis (np. zdjęcie), nr NIP, nr PESEL, seria i nr dowodu osobistego oraz stosunek do służby wojskowej.

# Załącznik nr 5 Opis przepływu danych osobowych

## Przepływ danych kadrowych (*na wzór)*

Pracownik Działu kadrowego

Pracownicy Działu księgowości

System płacowy

Kartoteka

Dane płacowe

Dane kadrowe

Przepływ   
danych

# Załącznik nr 6 Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

Przetwarzanie danych osobowych przez ………………..przy ul. …………………., i następuje w następujących pomieszczeniach:

1. Stacje robocze, na których przetwarzane są dane osobowe znajdują się w ……………… dedykowanych pomieszczeniach o numerach………………………………………..
2. Pomieszczenia, w których przechowywane są sprawne oraz uszkodzone elektroniczne nośniki informacji, kopie zapasowe zlokalizowane są w pokoju nr ………………….
3. Pomieszczenia, w których przechowuje się dokumenty źródłowe oraz wydruki z systemu informatycznego zlokalizowane są w pokojach nr …………………………………..
4. Kartoteki papierowa zawierające zbiory nieinformatyczne umiejscowione są w trzech pomieszczeniach o nr…………………….

)